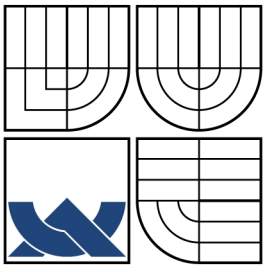
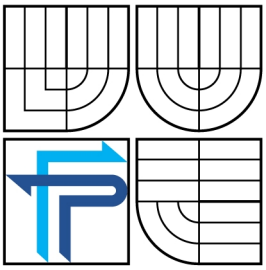


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUT OF INFORMATICS

PROBLEMATIKA BEZDRÁTOVÝCH SÍTÍ

WIRELESS FIDELITY NETWORKS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — VÍTĚZSLAV JÄGER
AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. MILOŠ KOCH, CSc.
SUPERVISOR

BRNO 2009

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2008/2009
Ústav informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jäger Vítězslav

Manažerská informatika (6209R021)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává bakalářskou práci s názvem:

Problematika bezdrátových sítí

v anglickém jazyce:

Wireless Fidelity Networks

Pokyny pro vypracování:

Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současné situace
Vlastní návrhy řešení, přínos návrhů řešení
Závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

Zandl,P.: Bezdrátové sítě WiFi : praktický průvodce. Vyd. 1. Brno : Computer Press, 2003. 190 s. ISBN 80-7226-632-2
Barken,L.: Wi-Fi : jak zabezpečit bezdrátovou síť. Vyd. 1. Brno : Computer Press, 2004. 174 s. ISBN 80-251-0346-3
Brisbin, Shelly. Wi-fi : postavte si svou vlastní wi-fi síť.Praha: Neocortex, 2003. 248 s. ISBN 80-86330-13-3
MOLNÁR, Z. Efektivnost informačních systémů. 1. vyd. Praha: Grada, 2000. 142 s. ISBN 80-7169-410-X.75.

Vedoucí bakalářské práce: doc. Ing. Miloš Koch, CSc.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2008/2009.

L.S.

Ing. Jiří Kříž, Ph.D. Ředitel ústavu	doc. RNDr. Anna Putnová, Ph.D., MBA Děkan fakulty

V Brně, dne 19.04.2009

Anotace závěrečné páce

Obsahem mé práce je uvést základní problematiku bezdrátových sítí. Podává přehled o používaných standardech. Analyzuji nejrozšířenější z nich a zaměřuji se na jejich architekturu a bezpečnost. Dalším krokem bude vytvoření bezdrátové sítě pro potřeby střední školy.

Anotation

Purpose of my Bachelor‘s thesis is to inform about general problems of wireless networks. My work is an overview about using standards. It analyzes the most common of them and focuses on their architecture and safety. Part of my work will be a creation of the wireless network for needs of a high school.

Klíčová slova

WiFi, IEEE 802.11, WiMax, WLAN, WEP, WPA, WPA2, bezdrátové sítě, bezpečnost bezdrátových sítí, architektura WLAN, SSID

Keywords

WiFi, IEEE 802.11, WiMax, WLAN, WEP, WPA, WPA2, wireless networks, security of wireless networks, architecture of WLAN, SSID

Bibliografická citace práce

JAGER, V. *Problematika Bezdrátových sítí*. Brno: VUT v Brně, Fakulta podnikatelská, 2009. 49 s. Vedoucí bakalářské práce: doc. Ing. Miloš Koch, CSc

Poděkování

Tímto bych rád poděkoval panu doc. Ing. Miloši Kochovi, CSc., vedoucímu této bakalářské práce, za jeho přínosné rady a užitečnou metodickou pomoc, které jsem využil při zpracování bakalářské práce.

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 15. května 2009

Vítězslav Jäger

OBSAH

1 ÚVOD

Když se v dnešní době řekne bezdrátová síť, téměř každý člověk v České republice zřejmě ví, o co se jedná a mnoho z nás se s ní setkává denně v praxi. Dříve byla bezdrátová síťová infrastruktura výsadou některých velkých firem a nebo nějakých internetových providerů. Pořizovací cena bezdrátové sítě byla příliš vysoká oproti klasické metalické kabeláži a také její rychlost nebyla dostatečná. Avšak v dnešní době ceny těchto zařízení jsou na takové úrovni, že se bezdrátové řešení sítě objevuje stále častěji i v menších firmách, pro které poskytují žádaný přínos. Umožňuje zaměstnancům přístup k systémových datům kdekoliv v dosahu sítě, když jsou data zapotřebí. Pokud by firma uvažovala například o rozšíření sítě do vedlejší budovy, je bezdrátová síť jedno z možných řešení. U metalických infrastruktur vznikají v praxi v mnoha případech problémy se samotným vedením kabeláže. Například vedení metalické kabeláže z jedné budovy do druhé, která je na druhé straně frekventované silnice, je velice nákladné a ve většině případů by firma ani od příslušných úřadů nedostala povolení. U bezdrátových sítí tyto problémy odpadají. Vývoj cen Wi-Fi hardwaru však umožnil proniknutí této technologie i do obyčejných domácností a pokud člověk vlastní přijímač bezdrátového signálu a projde se po ulici, není žádný problém nalézt mnoho signálů těchto sítí.

Bohužel s rozšiřováním této technologie si řada lidí vůbec neuvědomuje rizika – v praxi není problém se připojit přes bezdrátovou síť neopatrného majitele a přijímat od něj data. Pokud jde o domácí síť, mnozí lidé si myslí, že není důvod k opatrnosti. Své chování odůvodňují slovy: „Vždyť žádná užitečná data pro útočníka nevlastníme.*"* Ale opak je pravdou. Například využívání internetového bankovnictví z domu je stále častější. Prozrazení hesla může potenciálně způsobit ztrátu velkého finančního obnosu. A v oblasti firem je problém ještě kritičtější. Firma si nemůže dovolit, aby nějaký útočník zjistil strategická data z její databáze. Proto zabezpečení je jeden z klíčových aspektů bezdrátových sítí a bude mu věnována kapitola č.3.

2 CÍLE PRÁCE

- Informovat o standardech a jiných termínech používaných v oblasti Wi-Fi sítí.
- Podat přehled o existujících zabezpečujících mechanismech používaných v současnosti, upozornit na jejich výhody, ale i nevýhody.
- Navrhnout jaké řešení a jaký stupeň zabezpečení s ohledem na cenu a celkovou bezpečnosti sítě zvolit pro daný segment trhu.
- Přejít k tvorbě vlastní sítě, vysvětlit důvod jejího vzniku, následného využití a prakticky ukázat problémy, na které se v praxi naráží.

3 TEORETICKÁ VÝCHODISKA PRÁCE

3.1 Důvod vzniku jednotného standardu IEEE 802.11

Před znikem normy pro bezdrátové sítě IEEE[1] (Institute of Electrical and Electronics Engineers) 802.11 se musel pro tvorbu bezdrátové sítě vždy používat hardware od jednoho výrobce. Různé normy a specifikace jednotlivých výrobců neumožňovaly větší rozšíření bezdrátových sítí a z tohoto důvodu začala v roce 1990 organizace IEEE vytvářet normu, která by umožnila sestavit bezdrátovou síť i ze zařízení od různých výrobců. [1]

3.2 Standard IEEE 802.11

První standard rodiny 802.11 byl vytvořen v roce 1997, dnes je znám také pod názvem „802.11 legacy". Protokol pokrýval fyzickou a linkovou vrstvu modelu ISO/OSI. Tento standard využíval bezlicenční pásmo od 2,4 do 2,4835 GHz o rychlostech 1 Mbit/s nebo 2 Mbit/s.

Na fyzické vrstvě byly definované tři metody pro přenos dat. Dvě z nich využívaly metodu přenosu radiového signálu (FHSS a DSSS), třetí využívala infračervený přenos. [6]

3.2.1 FHSS

FHSS (Frequency Hopping Spread Spektrum) je vytvořeno na principu přeskakování frekvencí. Pásmo 2,4 GHz se rozdělí na nezávislé kanály o šířce 1 MHz. Během komunikace se tyto kanály střídají, na každém se vysílá maximálně 400 ms. Ve stejném pásmu může být provozováno až 20 přístupových bodů. Bohužel velikou nevýhodou tohoto řešení je nízká přenosová rychlost (maximálně 2 Mbit/s). [6]

[1]Institute of Electrical and Electronics Engineers [online]. 2008 [cit. 2009-05-04]
Dostupný z WWW: <http://standards.ieee.org>

3.2.2 DSSS

DDDS(Direct Sequence Spread Spectrum) je založeno na použití 13 kanálů o šířce pásma 22 MHz. Bezlicenční pásmo má šířku pouze 83,5 MHz. Realita je taková, že se dají použít pouze tři kanály, protože překrývající kanály se ruší. Takže v jedné lokalitě mohou pracovat pouze tři Wi-Fi sítě bez vzájemného rušení. [6]

3.2.3 Infračervený přenos

I když byl infračervený přenos ve standardu 802.11 definován, dodnes se nenašel žádný významný komerční produkt, který by infračerveného přenosu využíval. Infračervený přenos je velmi odolný proti rádiovému rušení, protože operuje s frekvencí v řádu THz. Jeho hlavní nevýhoda spočívá v omezeném dosahu a také v neschopnosti procházet zdmi. V době kdy vznikal standard 802.11, se všeobecně předpokládalo, že dojde k masivnímu rozšíření této technologie. Hlavní výrobci na trhu však přišli s masovou produkcí radiových adaptérů, následoval pád jejich cen a vítězství nad infračerveným přenosem. [6]

3.3 Rodina standardů IEEE 802.11

3.3.1 IEEE 802.11a

V roce 1999 byly schváleny dva doplňky standardu 802.11. První z nich nese název 802.11a. Od 802.11 se odlišuje tím, že pracuje v pásmu 5 GHz. Přenosová rychlost je výrazně vyšší, dosahuje 54 Mbit/s. Tento standard zavádí poprvé modulaci OFDM (Orthogonal Frequency Division Multiplexing). Frekvenční pásmo je rozděleno na mnoho úzkých kanálů, kterými jsou data přenášena současně. Mezi nevýhody tohoto standardu patří především to, že nedokáže komunikovat se zařízeními používající standard 802.11b a jeho následovníky. [17]

3.3.2 IEEE 802.11b

IEEE 802.11b je druhý ze standardů schválených v roce 1999. Pracuje v pásmu 2,4 GHz. Oproti původnímu standardu 802.11 dosahuje vyšší rychlosti až 11 Mbit/s. 802.11b Využívá pro přenos dat už pouze technologii DSSS tzn. zpětná kompatibilita s kartami, které používaly technologii FHSS, už není zajištěná. Ve špatných podmínkách, například v důsledku silného zarušení frekvenčního pásma, používá 802.11b principu dynamické změny přenosové rychlosti. Ve špatných podmínkách může rychlost klesnout. Může se snížit na 5,5 Mbit/s nebo dokonce 1-2 Mbit/s, při zlepšení těchto podmínek se zase rychlost vrací na maximálních 11 Mbit/s. Tento standard se stal velice oblíbeným díky dvěma hlavním faktorům. Za prvé díky relativně nízkým pořizovacím nákladům, za druhé díky pomoci Wi-Fi aliance[2], které se úspěšně podařilo zajistit kompatibilitu zařízení od různých výrobců. [17]

3.3.3 IEEE 802.11g

Standard 802.11g byl schválen v roce 2003. Opět využívá pásmo 2,4 GHz. Přenosová rychlost dosahuje až 54 Mbit/s. Pro takové zvýšení rychlosti byla na fyzické vrstvě použita technologie OFDM (Orthogonal Frequency Division Multiplexing), která se objevila už u 802.11a. Pro zajištění zpětné kompatibility s 802.11b je zde použita i technologie DSSS. V případě, že všichni připojení klienti mají wi-fi adaptér podporující standard 802.11g, je teoretická rychlost již uvedených 54 Mbit/s. Pokud se však připojí klient s podporou pouze 802.11b, rychlost celé sítě se rapidně sníží. Standard 802.11g se stal jedním z nejrozšířenějším vůbec a drtivá většina současných bezdrátových karet využívá těchto specifikací. [17]

3.3.4 IEEE 802.11n

Vývoj IEEE 802.11n se datuje k roku 2003, protože bylo jasné, že ani zvýšená rychlost 802.11g nebude v brzké době dostačující. Jasným cílem bylo vyrovnat se a v lepším případě i překonat v té době nejčastěji používaný Ethernet, který dosahoval rychlosti 100 Mbit/s. Avšak datum jeho dokončení se odkládá už několik let. V roce

[2] Wi-Fi Alliance [online]. 2008 [cit. 2009-05-04]
Dostupný z WWW: <http://www.wi-fi.org>

2008 byl představiteli aliance určen termín dokončení na březen 2009. V době psaní této práce, duben 2009, tento standard není stále úplně dokončený a poslední informace hovoří o listopadu 2009. Nicméně na trhu můžeme koupit již celou řadu zařízení, která podporují zatím nejnovější verzi 802.11n Draft 2.0.

Standard 802.11n je schopen výrazně zvýšit přenosovou rychlost bezdrátové sítě. Teoretická rychlost dosahuje 300 Mbit/s, reálná rychlost je okolo 130 Mbit/s, což je významný krok kupředu. Je použita nová technologie MIMO (Multiple- Input Multiple-Output) nebo také technologie tzv. „chytrých antén". Pracuje na principu vysílání několika signálů různými cestami, díky použití více antén jak u vysílače tak u přijímače.

Velkou výhodou je zpětná kompatibilita s 802.11b/g, což umožňuje postupné zařazování těchto zařízení do běžného provozu v dnešních bezdrátových sítích.

Avšak použití několika kanálů současně pro zvýšení přenosové rychlosti s sebou přináší i nevýhody. Malý počet kanálů v bezlicenčním pásmu v praxi často nedovoluje využití několika kanálů současně a proto reálná rychlost je mnohdy výrazně nižší, než jaká by mohla za dobrých podmínek být. [7]

3.4 Struktura Wi-Fi sítí

3.4.1 Režim ad-hoc

Režim ad-hoc neobsahuje žádný přístupový bod (AP - Access Point), ale koncové stanice jsou propojeny a komunikují přímo mezi s sebou. Bezdrátový charakter přenosu dat umožňuje propojení více než dvou koncových uživatelů, avšak ne ve stejném čase. Režim ad-hoc si lze představit jako komunikaci „po dvojicích", bez použití prostředníka. Toto schéma je vhodné pro síť o několika stanicích, které jsou vzdálené od sebe několik metrů. Většinou takovéto sítě vznikají pro nějaký specifický účel, například výměnu dat mezi uživateli. Až splní svůj účel, síť zaniká. Režim ad-hoc velkou oblibu nezískal z důvodu omezenosti rozsahu sítě a také nutnosti specifické konfigurace sítě. [18]

3.4.2 Režim infrastruktury

V infrastrukturních sítích je komunikace mezi uživateli zprostředkována přes přístupový bod AP (Access point). AP umožňuje komunikaci bezdrátových zařízení v jeho dosahu a vytváří infrastrukturu sítě.

Pokud nějaká stanice chce komunikovat s nějakou další v síti, přenos dat probíhá ve dvou částech. Nejdříve jsou data odeslána na přístupový bod a z něj jsou potom poslána na adresovanou stanici.

Režim infrastruktury se rozděluje na dva typy. První typ je BSS (Basic Service Set) - síť se skládá pouze z jednoho přístupového bodu, ze kterého je pak dále signál šířen k uživatelům. Můžeme tak například vytvořit malou síť v domácnosti nebo v nějaké kanceláři.

Pokud bychom propojili páteřní sítí dvě a více sítí BSS dostáváme druhý typ sítě a to sít ESS (Extended Service Set). [1]

3.4.3 Bezdrátové přemostění sítě

Bezdrátové přemostění sítě je speciální režim AP, který umožňuje spojit (přemostit) dvě a více sítí. Pokud tento režim na zařízení nastavíme, přestává už fungovat jako AP, který by umožňoval klientům přímý bezdrátový přístup do sítě.

3.4.3.1 Point to Point (PTP)

Máme dvě oddělené sítě LAN a chceme je propojit, například každá síť je umístěná v jiné budově. Jedna z možností je použít dva AP v módu PTP. Vytvoříme tak bezdrátový most mezi těmito dvěmi sítěmi. Avšak pokud AP použijeme v módu PTP, uživatelé se již nemohou připojovat na tyto AP. Pokud bychom chtěli mít v budovách i bezdrátovou infrastrukturu, museli bychom do návrhu začlenit přístupové body, které by byly vyhrazeny pro připojování klientů. [6]

3.4.3.2 Point to Multipoint (PTMP)

Je to obdoba módu Point to Point s tím rozdílem, že nepřipojujeme pouze dvě sítě, ale k jedné síti jich připojíme hned několik. Zde bohužel panuje velká nejednotnost

mezi výrobci, a proto při výstavbě této sítě se doporučuje použít zařízení pouze od jednoho výrobce. Projevila se zde benevolentnost standardu IEEE 802.11, která umožnila mnoho řešení od různých výrobců nekompatibilních mezi sebou. Opět zde platí, že zařízení použitá v módu PTMP není možné zároveň využívat jako AP pro připojování klientů. [6]

3.4.3.3 Bezdrátový opakovač (repeater)

Funkce opakovače je taková, že opakuje (zesiluje) signál z určitého přístupového bodu a tím zvětšuje jeho dosah. Je to specifické řešení a najde využití především u poskytovatelů bezdrátového internetu, kteří jsou přírodními podmínkami (např. kopcovitým terénem) nuceni zesilovat signál. [6]

3.4.3.4 Master plus AP

Tento mód je velice specifický. Jeho výhoda spočívá v tom, že dokáže přemostit jak připojení (PTMP), tak je zároveň schopen poskytovat bezdrátové připojení pro uživatele. Jeho cena však nedovoluje nějaké plošné využití a používá se jen ve speciálních případech, kdy například velký radiový provoz v oblasti nedovoluje využít dvě bezdrátové zařízení pracující v bezlicenčním pásmu ve stejné oblasti. [6]

3.5 Zabezpečovací mechanismy Wi-Fi sítě

Na rozdíl od metalických sítí se u bezdrátových sítí šíří signál i mimo námi požadovaný prostor, bez ohledu na zdi, či jiné překážky. Při koupi nového bezdrátového zařízení zjistíme, že zde není nastavena žádná ochrana.

Bezpečnost bezdrátových sítí je opravdu velmi rozsáhlé téma, existuje mnoho způsobů jak zabezpečit bezdrátovou síť, bohužel existuje i velký počet útoků na tyto zabezpečení.

3.5.1 SSID

Jedno z častých zabezpečení je skrytí identifikátoru sítě SSID (Service Set Identifier). Běžně je tento identifikátor vysílán AP. Bez znalosti identifikátoru se nelze na síť připojit. SSID představuje klíč dlouhý až 32 znaků. Všechna bezdrátová zařízení, která chtějí spolu komunikovat musí mít znalost klíče SSID.

3.5.1.1 Zjištění SSID

Skrytí SSID neposkytuje téměř žádné zabezpečení. Dnes existuje mnoho programů (např. NetStumbler), které jsou schopny SSID zjistit, i když je jeho vysílání na AP zamezeno.

Existují dva druhy útoků

1. Pasivní: Útočník sleduje provoz v nějaké bezdrátové síti. Počká, až se nějaká stanice pokusí na tuto sít připojit, v tuto chvíli se mu podaří SSID bez problémů zjistit.
2. Aktivní: Útočník nečeká, než se nějaký klient připojí, ale vyšle odpojovací paket pro stávajícího uživatele a tím ho donutí k opětovnému přihlašování. A opět odposlechne SSID sítě.[10]

3.5.1.2 Ochrana proti zjištění SSID

Bohužel SSID nikdy nebylo navrženo jako bezpečnostní prvek sítě a také proto je implicitně nastaveno vysílání SSID. Efektivní ochrana proti zjištění neexistuje. Tento způsob ochrany je použitelný pouze např. v případě nenakonfigurované stanice, která ještě není využívána.

3.5.2 MAC adresa

MAC (Media Access Control) je jedinečný identifikátor síťového zařízení, který používají různé protokoly druhé (linkové) vrstvy modelu ISO/OSI. MAC adresa se skládá ze 48 bitů. V praxi je zapisována jako šestice dvojciferných hexadecimálních čísel oddělených pomlčkami (např. 01-23-45-67-89-ab)

MAC adresa přidělená výrobcem je vždy celosvětově jedinečná. Z hlediska přidělování je rozdělena na dvě poloviny. O první polovinu musí výrobce požádat centrálního správce adresního prostoru a je u všech karet daného výrobce stejná. Výrobce poté kartě či zařízení přiřadí jedinečnou hodnotu druhé poloviny MAC adresy. Jednoznačnost velmi usnadňuje správu lokálních sítí. Novou kartu lze zapojit a spolehnout se na to, že bude jednoznačně identifikována. [14]

3.5.2.1 Kontrola přístupu pomocí MAC adresy

Ve standardu 802.11 byl zaveden způsob kontroly přístupu pomocí filtrování MAC adres na straně AP. Pokud toto filtrování máme aktivní, asociace je úspěšná pouze tehdy, je-li zaznamenána adresa připojujícího se klienta v seznamu povolených MAC adres.

Dvě základní nevýhody tohoto zabezpečení:

1. Zadávaní MAC adres do seznamu a případná obměna je časově náročná i v malé síti.
2. Druhým nedostatkem je schopnost útočníka odposlechnout MAC adresu stanice, která se přihlašovala do systému a pomocí jednoduchého nástroje (např. MAC Spoofer[3]) si změnit MAC adresu svoji síťové karty na adresu síťové karty, která v seznamu AP je povolena. Poté už se útočník může v síti volně pohybovat.

3.5.3 Šifra WEP

Wired Equivalent Privacy (WEP) zajišťuje šifrování rámců na úrovni třetí (síťové) vrstvy modelu ISO/OSI. Šifruje veškeré rámce, které vedou od klienta k AP.

[3] MAC Spoofer [online]. 2006 [cit. 2009-05-04]
Dostupný z WWW: <http://www.soft-go.com/view/Mac-Spoofer_52.html>

K šifrovaní se používá algoritmus RC4[4], jehož autorem je R. Rivest a zveřejněn byl v roce 1994. Algoritmus používá symetrickou proudovou šifru s délkou klíče 40 nebo 104 bitů.

Šifrování probíhá operací XOR mezi zprávou a klíčovým řetězcem a dešifrování probíhá reverzně. WEP bohužel nijak neřeší distribuci klíče. Odesílatel i příjemce musí mít stejný klíč používaný k šifrování a dešifrování komunikace. Pro vyšší bezpečnost je nutné, aby byl klíč průběžně obměňován. To ale WEP nijak neřeší a tak jediný možný způsob změny klíče je opětovné nahrazení stávajícího v konfiguraci adaptéru. Avšak ruční zadávání klíče je naprosto nevhodné, protože případný útočník může nový klíč při předání získat.

Zašifrování stejné zprávy symetrickou šifrou pokaždé generuje stejnou šifrovanou zprávu. Proto WEP obsahuje ještě inicializační vektor (IV), který se mění s každým paketem a doplňuje klíč o dalších 24 bitů. Při použití WEP s klíčem dlouhým 64 bitů má klíč pouze 40 bitů , zbylých 24 tvoří inicializační vektor. Generování IV zajišťuje vysílací strana, která ho nejenom použije k sestavení šifrovaného řetězce, ale přidá ho v otevřené podobě i do záhlaví rámce. Tímto způsobem měl být klíč chráněn proti prozrazení. Bohužel existuje pouze 16 777 216 kombinací. Tato relativně malá množina inicializačních vektorů v praxi způsobí, že po určitém objemu přenesených dat se začnou opakovat. Inicializační vektor neposkytuje potřebné zabezpečení a šifra je napadnutelná řadou útoků. [20, 21, 24]

3.5.3.1 Nedostatky WEP

Šifrování:

- Je použit stejný klíč na všech zařízeních v síti - sdílený klíč
- Klíč je statický, neobměňuje se v čase
- Slabý šifrovací mechanismus RC4

[4] Proudová symetrická šifra RC4 [online]. 2004 [cit. 2009-05-04]
Dostupný z WWW: <http://en.wikipedia.org/wiki/RC4>

Autentizace:

- Absence oboustranné autentizace - uživatel si nemůže být jistý, zda se nepřipojuje k podvrženému přístupovému bodu
- Klíč je navržen tak, že nepodporuje autentizaci uživatele, pouze zařízení. V případě zcizení zařízení je klíč prozrazen (je nutné změnit klíče na všech stanicích)

3.5.4 802.1X

K pochopení standardu 802.1X je potřeba vysvětlit tři separátní pojmy: PPP, EAP a 802.1X. PPP (Point-to-Point Protocol) je jeden z nejvíce využívaných protokolů pro vytáčené připojení k internetu. PPP je také používán některými poskytovateli DSL a kabelového připojení k autentizaci. PPP se rozšířilo ze svého původního použití ve vytáčeném připojení a nyní je široce využíváno přes internet. Autentizace u PPP je využívána k identifikaci uživatele na konci linky PPP předtím, než je mu umožněn přístup.

Většina podniků chtěla mít větší zabezpečení, než pouze zadávání uživatelského jména a hesla pro přístup do sítě. A tak byl navržen nový autentizační protokol EAP (Extensible Authentication Protocol). EAP je implementován uvnitř autentizačního protokolu PPP a poskytuje obecný rámec pro několik jiných autentizačních metod.

Se standardem EAP se práce v oblasti síťové komunikace stala mnohem snadnější. Je pouze nutné, aby klient a autentizační server podporovaly EAP. IEEE 802.1X je standard pro komunikaci EAP přes metalickou a nebo bezdrátovou LAN. Využití má například v situacích, kde je použit jiný protokol než TPC/IP a nebo kde je nežádoucí komplexnost celého EAP.

802.1X užívá tři termíny se kterými se musíme seznámit. Uživatel nebo klient, který chce být autentizován, se nazývá žadatel. Aktuální server provádějící autentizaci, typicky RADIUS[5] (Remote Authentication Dial In User Service) server, se nazývá autentizační server a zařízení uprostřed, například access point, se nazývá autentizátor. Jedna z klíčových vlastností 802.1X je, že autentizátor nemusí být nijak složitý a sofistikovaný. Všechny výpočty provádí žadatel a autentizační server. Z tohoto

[5] RADIUS server [online]. 2008 [cit. 2009-05-04]
Dostupný z WWW: <http://freeradius.org>

důvodu je 802.1X ideálním pro použití u bezdrátových AP, které jsou typicky malé, mají malou paměť a nízký výpočetní výkon. [23]

3.5.4.1 LCP

Link-Control Protocol je použit ještě před tím, než je rozhodnuto o tom, jaký síťový protokol na lince poběží. LCP je společným protokolem pro všechny síťové protokoly. Protokol LCP má za úkol navázat spojení, ukončit spojení, výměnu autentizačních informací apod. Linka se nachází postupně ve stavu navazování spojení, autentizace a ukončování spojení. [3]

3.5.4.2 PAP

Password Authentication Protocol je obdobný jako autentizace pomocí terminálového dialogu. Uživatel prokazuje svou totožnost také pomocí jména a hesla. Pro výměnu autentizačních informací je však použit protokol LCP - uživatelské jméno a heslo není přímo vloženo na linku, ale je zabaleno do protokolu LCP. [3]

3.5.4.3 CHAP

Challenge Handshake Authentication Protocol je považovaný za dokonalejší než PAP a je mu v praxi dávána přednost. Oba koncoví účastníci komunikace sdílí stejný šifrovací klíč symetrické šifry (sdílené tajemství). Stanice, která podnítila k začátku autentizace, vygeneruje náhodný řetězec jako dotaz (challenge), který je odeslán druhé straně. Druhou stranou je tento řetězec zašifrován a odeslán zpět. Stanice, která iniciovala autentizaci, tak obdržela zašifrovaný řetězec. Poté vezme původní řetězec, zašifruje jej sama a porovná oba výsledky. Jsou-li totožné, pak protější straně potvrdí úspěšný výsledek autentizace. V opačném případě odpoví, že autentizace proběhla neúspěšně a je nutno začít znovu s navazováním spojení.

Výhodou protokolu CHAP je skutečnost, že obě komunikující strany vlastní stejný sdílený šifrovací klíč. Je tak snadné provádět autentizaci oboustranně. [3]

3.5.5 EAP

EAP[6] (Extensible Authentication Protocol) v současné době podporuje mnoho autentizačních technik. Liší se v náročnosti implementace a také v celkové bezpečnosti, kterou poskytují. Pro úspěšnou implementaci musí zvolenou metodu podporovat všichni tři účastníci komunikace - klient, autentizátor a také autentizační server. [8]

3.5.5.1 EAP-MD5

EAP-MD5 je nejjednodušší technika zabezpečení v EAP. Je použito pouze uživatelské jméno a heslo. EAP-MD5 chrání přenos informací vytvořením unikátního digitálního podpisu ke každému paketu, aby bylo zajištěno, že zprávy EAP jsou pravé. Protokol EAP-MD5 není nikterak náročný a provádí své operace velmi rychle. Z tohoto důvodu není jeho implementace v síti složitá. [8]

Nedostatky EAP-MD5

Neověřuje totožnost klienta, neposkytuje silné šifrování pro digitálně podepsané zprávy poslané mezi klientem a autentizačním serverem. Protokol EAP-MD5 je zranitelný proti slovníkovým útokům i útokům typu „man-in-the-middle". EAP-MD5 je vhodný pro kabelové sítě, kde je EAP klient přímo spojen s autentizátorem a šance narušení komunikace nebo změna zprávy je velice malá. Pro autentizaci 802.1X bezdrátových sítí jsou používány silnější EAP autentizační protokoly. [8]

3.5.5.2 EAP-TLS - Transport Level Security

Poskytuje jedno z nejsilnějších zabezpečení, avšak zároveň jeho implementace je jedna z nejsložitějších. Klient i autentizační server se identifikují za použití digitálních certifikátů podepsaných certifikační autoritou. Poskytuje vzájemnou autentizaci mezi klientem a serverem a je velmi bezpečný. EAP zprávy jsou zabezpečeny proti odposlouchávání TLS tunelem, který je vytvořen mezi klientem a autentizačním serverem. Velkou nevýhodou EAP-TLS je vyžadování certifikátů na straně klienta i serveru - správa sítě musí být mnohem více komplexní a tím pádem

[6] Extensible Authentication Protocol [online]. 2004 [cit. 2009-05-04]
Dostupný z WWW: <http://www.ietf.org/rfc/rfc3748.txt>

i dražší. EAP-TLS je vhodné pro implementaci tam, kde již existuje infrastruktura s certifikační autoritou. TLS se nejčastěji používá v bezdrátových infrastrukturách. [8]

3.5.5.3 EAP-TTLS - Tunneled Transport Level Security

EAP-TTLS podporuje výhody silného zabezpečení jako u EAP-TLS, avšak bez nutnosti oboustranné certifikace na straně klienta a serveru. Podporuje stejně jako EAP-TLS vzájemnou autentizaci, avšak pouze autentizační server musí být ověřen nezávislou certifikační autoritou. Klienti se mohou autentizovat pomocí uživatelského jména a hesla. Pro autentizační server je vyžadován certifikát. EAP-TTLS snižuje náklady potřebné na údržbu sítě, přičemž síť je dobře zabezpečená. Je zde zajištěna zpětná kompatibilita s autententizačními protokoly jako například PAP (Password Authentication Protocol) a CHAP (Challenge Handshake Authentication Protocol). EAP-TTLS není považován jako naprosto bezpečný a jde přelstít v případě, když při ověřování identity klienta není použito bezpečného komunikačního kanálu. EAP-TLS se používá v případech, kdy je zapotřebí velké bezpečnosti bez použití oboustranných certifikátů. [8]

3.5.5.4 PEAP - Protected EAP

PEAP je internetová obdoba EAP-TTLS, kterému se podobá ve smyslu funkcí oboustranné autentizace. V dnešní době je prosazován různými firmami (Microsoft, Cisco) jako alternativa právě k EAP-TTLS. Spoléhá na již vytvořenou metodu vytváření a výměny klíčů TSL. PEAP klient se autorizuje přímo s autentizačním serverem, autentizátor pouze přeposílá komunikaci a není u něj vyžadována podpora specifických EAP autentizačních protokolů. Na rozdíl od EAP-TTLS, PEAP nepodporuje kontrolu uživatelského jména a hesla s existující databází. PEAP je vhodný pro instalaci do míst, kde jsou vyžadována přísná pravidla pro autentizaci bez použití oboustranných certifikátů. [8]

3.5.5.5 Cisco Lighweight EAP

Byl vytvořen v listopadu roku 2000 pro vyřešení problémů v oblasti bezpečnosti bezdrátových sítí. LEAP je forma EAP, která vyžaduje oboustrannou autentizaci mezi klientem a autentizátorem. Nejdříve se klient musí autentizovat autentizátoru a poté se autentizátor autentizuje klientovi. Pokud obě autentizace proběhnou úspěšně, je navázáno síťové připojení. Na rozdíl od TLS, LEAP je založeno na uživatelském jménu a heslu a nevyužívá certifikátů od certifikační autority. Nevýhoda tohoto řešení spočívá v tom, že je to řešení jediné firmy Cisco, která neumožnila ostatním společnostem tento protokol poskytovat. LEAP je vhodný pro řešení bezdrátové sítě, která využívá komponenty pouze od společnosti Cisco. [8]

3.5.5.6 Přínos EAP

Umožňuje podporu mnoha autentizačních protokolů bez nutnosti mít předem nějaký společný dohodnutý. Jeho flexibilita dovoluje autentizátoru podporovat mnoho autentizačních protokolů bez specifických znalostí jejich autentizačních mechanismů. Díky EAP pouze autentizační server kontroluje, které autentizační mechanismy jsou použité mezi ním a klientem. Autentizátor zde pouze plní funkci předávače informací pro potřeby serveru a klienta.

3.5.5.7 TKIP

Temporal Key Integrity Protocol využívá stejného šifrovacího algoritmu jako WEP, používá standardně 128 bitový klíč, ale na rozdíl od WEP obsahuje dočasné klíče. TPIK pracuje s automatickým klíčovým mechanismem, který mění dočasný klíč každých 10 000 paketů. Další velkou výhodou TKIP je Message Integrity Check (MIC), tedy kontrola integrity zpráv. MIC je podstatně lepší zabezpečení integrity zpráv než před ním používaný jednoduchý kontrolní součet CRC. MIC má za úkol znemožnit útočníkům změnu zprávy po přenosu.[11]

3.5.5.8 MIC

U standardu 802.11 a šifrování WEP je integrita dat zajišťována pomocí 24 bitové hodnoty IVC (Integrity Check Value), která je připojena k datové části a zašifrována metodou WEP. Chyba této kontroly integrity umožňuje útočníkovy změnit specifické bity v datové části a aktualizovat šifrovanou hodnotu ICV, aniž by to tato kontrola byla schopná detekovat. Této chyby je využito v útocích na zabezpečení WEP.

U standardu WPA je použita nová metoda označovaná jako Michael. Je to nový algoritmus, který pomocí výpočetních možností bezdrátových zařízení vypočte osmi bajtový kontrolní součet MIC (Messege Integrity Check). MIC je umístěn mezi datovou část rámce IEEE 802.11 a čtyřbajtovou hodnotu ICV. Pole kontrolního součtu je zašifrováno společně s daty rámce a hodnotou ICV. [11]

3.5.6 WPA2

V roce 2004 byl schválen dodatek 802.11i, někdy označovaný také jako WPA2, který zcela nahrazuje WEP. Hlavní rozdíl mezi WPA a WPA2 je v tom, že WPA2 přináší blokovou šifru AES[7] (Anvanced Encryption Standard). Možnost využití TKIP je ponechána pro zachování zpětné slučitelnosti s WPA.

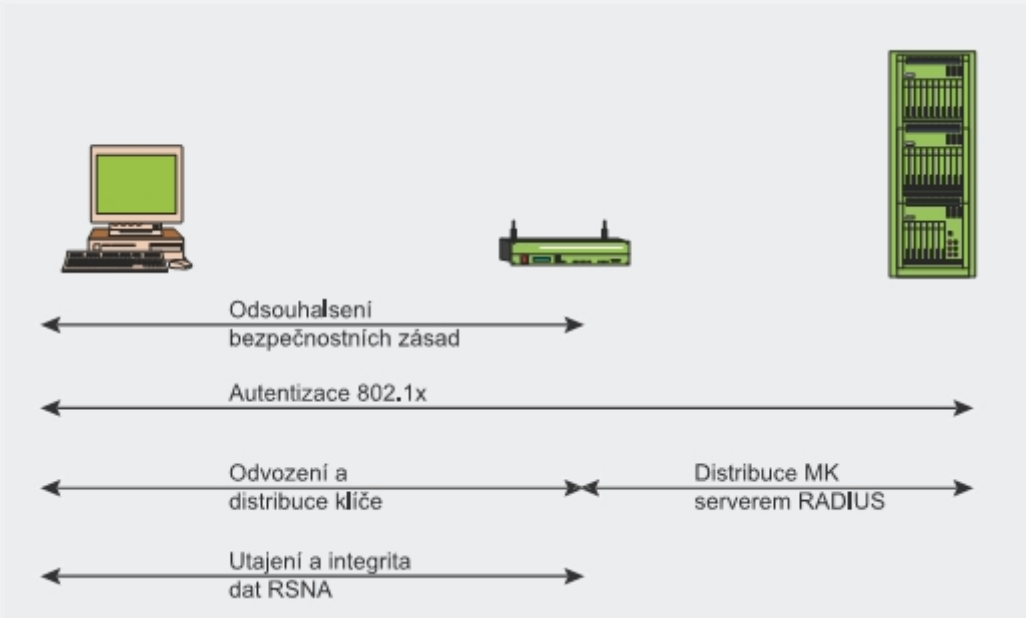
Z důvodů nedostatečné bezpečnosti WEP byl sestaven tým za účelem uvést nový bezpečnostní standard, který by byl schopen zvýšit bezpečnost přenášených dat a zlepšit šifrování standardu 802.11. Ze strany výrobců síťových zařízení byl vznesen požadavek na zpětnou kompatibilitu, protože zákazníci by si zřejmě nebyli ochotni měnit svá stávající zařízení. V červnu roku 2004 byla schválena poslední verze standardu 802.11i, který byl asociací Wi-Fi Aliance pojmenován WPA2. WPA2 přináší základní změny jako například oddělení autentizace a kontrolu integrity zprávy. Tím pádem je schopný poskytnout stabilní a flexibilní bezpečnostní architekturu, která je použitelná nejen pro malou domácí síť, ale i pro rozsáhlé podnikové sítě. Nová architektura zabezpečení bezdrátových sítí nese název RSN (Robust Security Network) a využívá autentizaci podle 802.1X. Je zde používán bezpečný mechanismus pro distribuci klíčů a jsou zde nové mechanismy sloužící k zajištění bezpečnosti a integrity v celé síti. RSN je oproti

[7] Šifra AES [online]. 2008 [cit. 2009-05-04]
Dostupný z WWW: <Zdroj: www.ietf.org/rfc/rfc3268.txt>

předchozí architektuře složitější, avšak nabízí škálovatelná a bezpečná řešení pro bezdrátovou komunikaci. I když zařízení RSN ve většině případů akceptuje pouze zařízení opět s podporou RSN, v IEEE 802.11i je definována i architektura TSN (Transitional Security Network), který je schopen obsáhnout jak RSN, tak i systémy WEP. Asociace je označena jako RSNA (Robust Security Network Association). [11]

3.5.6.1 4 fáze zabezpečení u WPA2

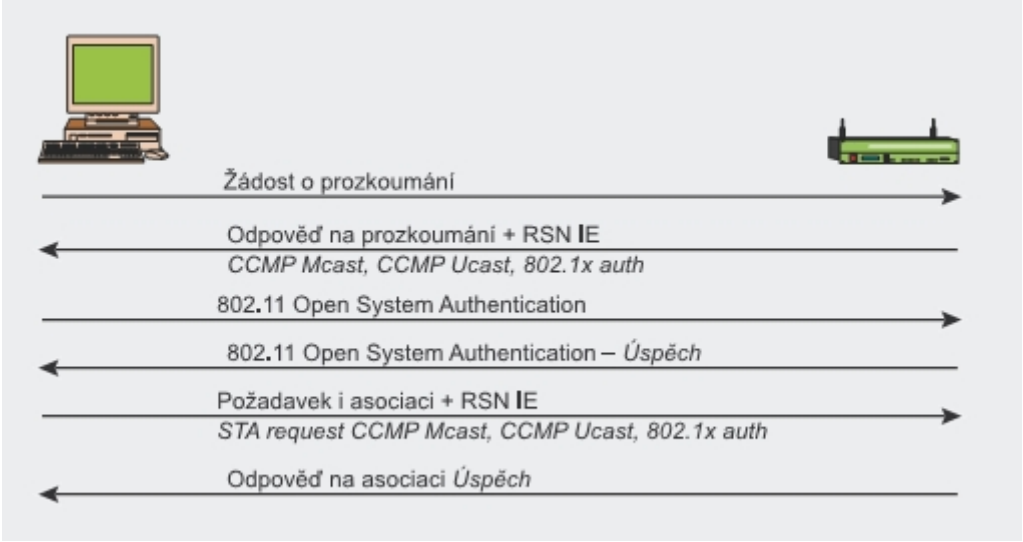
- Odsouhlasení bezpečnostních zásad
- Autentizace podle 802.1X
- Odvozování a následná distribuce klíčů
- Utajení a integrita dat v RNSA



Obrázek 3.1: Fáze standardu 802.11i, převzato z [11]

Fáze 1: Odsouhlasení bezpečnostních zásad

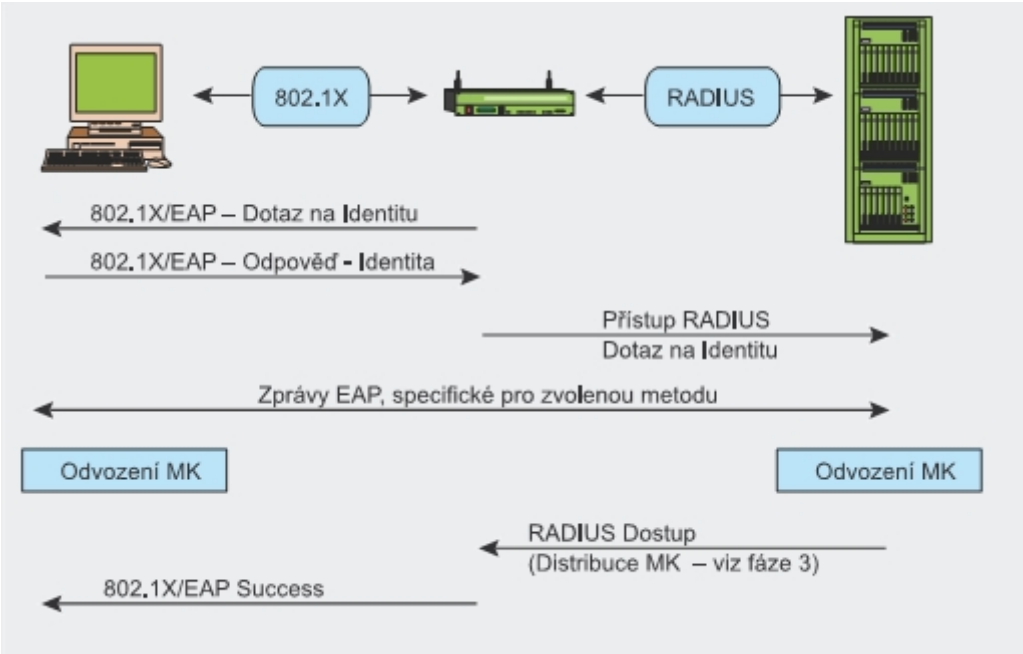
V první fázi je nutné, aby se komunikující strany shodly na určitých bezpečnostních zásadách, které budou využívat.



Obrázek 3.2: Fáze 1: Odsouhlasení bezpečnostních zásad, převzato z [11]

Fáze 2: Autentizace podle 802.1X

Zde probíhá autentizace založená na protokolu EAP. Autentizace 802.1X je zahájena, když jsou přístupovým bodem vyžadovány údaje obsahující klientovu identitu. Dále proběhne výměna zpráv mezi autentizačním serverem a klientem, aby mohl být vygenerován společný Master Key (MK). Na konec této procedury je vyslána zpráva Radius Accept, která obsahuje MK a konečnou právu EAP Success pro klienta.

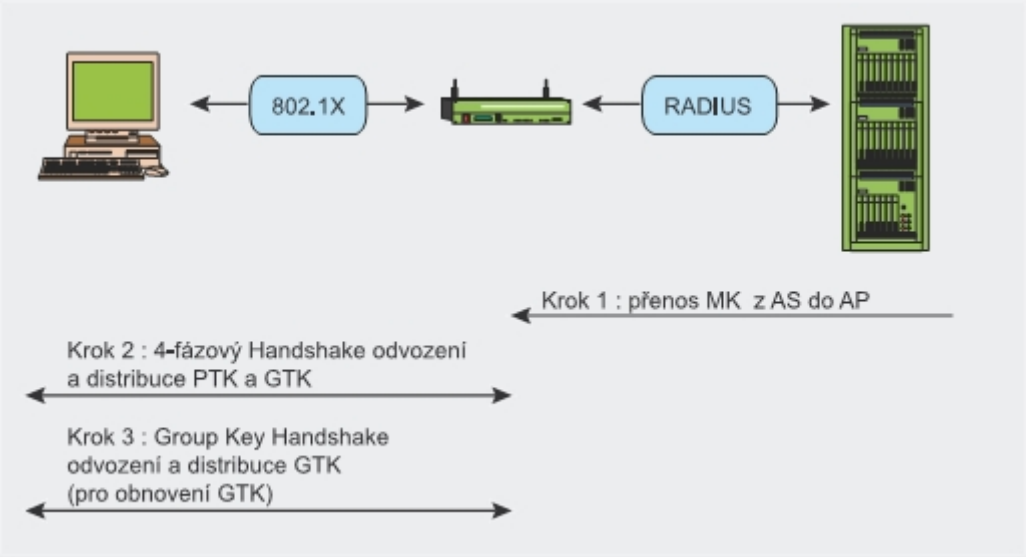


Obrázek 3.3: Fáze 2: Autentizace podle 802.1X, převzato z [11]

Fáze 3: Odvození a distribuce klíčů

Zabezpečení klíčů je jeden ze základních prvků k zabezpečení celé sítě. V architektuře RSN je životnost klíče omezena. Celkové zabezpečení se zde zajišťuje pomocí různých klíčů, jež jsou uspořádány hierarchicky. Jakmile je po úspěšné autentizaci stanoven bezpečnostní kontext, jsou vytvořeny dočasné (relační) klíče, které jsou pravidelně aktualizovány, dokud není bezpečnostní kontext uzavřen. Výměna a generování klíčů je hlavní úkol fáze 3. V průběhu odvozování klíče je zapotřebí dvou „podání rukou" mezi klientem a RADIUS serverem. Prvního čtyřstranného podání rukou mezi klientem a RADIUS serverem pro odvození PTK (Pairwise Transient Key) a GTK (Group Transient Key). A druhého pro obnovení GTK. Odvození PMK (Pairwise Master Key) je závislé na použité autentizační metodě. [11]

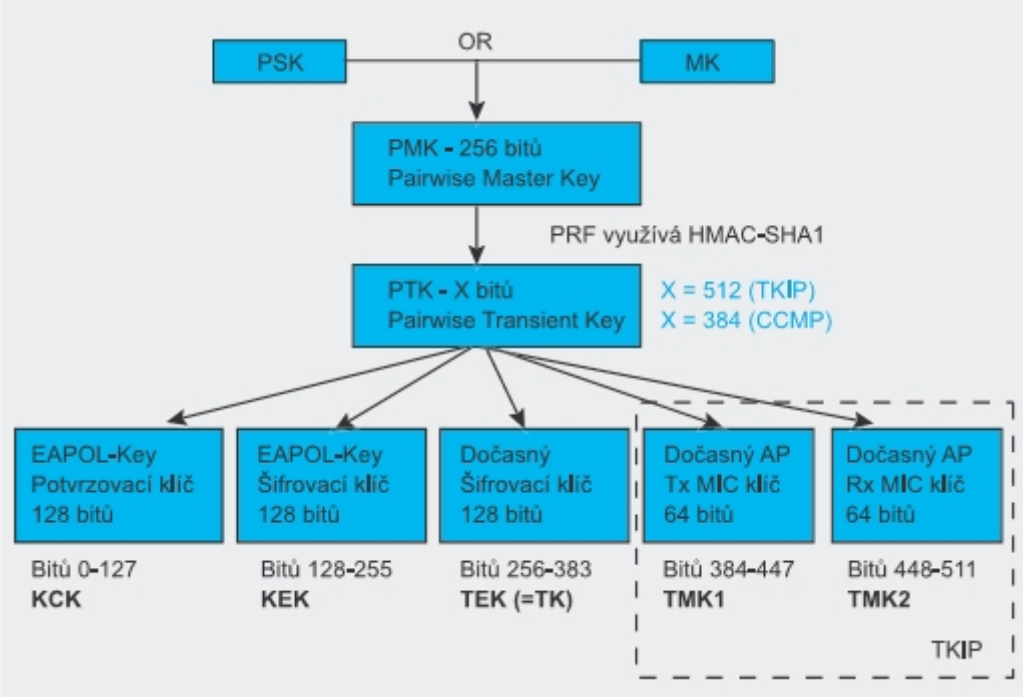
- První metoda poskytuje řešení pro menší sítě (malé podniky, domácnosti), které nevlastní autentizační server. Je zde použit PSK (Pre-Shared Key), PMK = PSK. PSK je vygenerován z hesla, které je tvořeno z více slov či shluků znaků v rozmezí od 8 do 63 znaků nebo 256 bitového řetězce.
- Je-li použit autentizační server, PMK je odvozen v průběhu autentizace 802.11X MK. Tato metoda bude vysvětlena níže.



Obrázek 3.4: Fáze 3: Odvození a distribuce klíčů, převzato z [11]

Samotný PMK však nikdy není použit k šifrování nebo kontrole integrity dat. Jeho úkol spočívá v generování dočasného šifrovacího klíče PTK. Délka PTK se odvíjí od šifrovacího protokolu. PTK je složen z několika dočasných klíčů.

- KCK (Key Confirmation Key) - jeho délka je 128 bitů a slouží k autentizování zprávy během čtyřstranného podání rukou.
- KEK (Key Encryption Key) - jeho délka je opět 128 bitů. Klíč pro utajení dat během zajišťování PTK a GTK.
- TK (Temporary key) - délka 128 bitů. Je použit pro zašifrování dat u TKIP (Temporal Key Integrity Protocol) a CCMP (Cipher Block Chaining Message Authentication Code Protocol)
- TMK (Temporary MIC Key) - délka 2x64 bitů. Slouží k autentizaci dat.



Obrázek 3.5: Hierarchie klíčů v 802.11i, převzato z [11]

Čtyřstranné podání rukou umožňuje:

- Šifrovat přenos GTK
- Potvrdit, že klient má znalost PMK
- Instalovat klíče pro šifrování a integritu
- Potvrdit výběr sady šifer

Fáze 4: Utajení a integrita dat v RSNA

Je zde použit protokol TKIP. Ten přináší opravy ke zranitelným místům WEP:

- Pro integritu zpráv je zde použit nový protokol MIC (Message Integrity Protocol), který lze implementovat i na software běžících na pomalých mikroprocesorech.
- Nová výběrová pravidla pro hodnoty iniciačního vektoru: V rámci zamezení opětovného použití IV je zvětšena jeho velikost.
- Je implementována správa klíčů, nový mechanismus pro sdílení a následnou distribuci klíčů.[11]

3.5.6.2 AES

AES (Advanced Encryption Standard) je šifrovací algoritmus, který je v současnosti používán v civilním i vojenském sektoru pro ochranu nejcitlivějších informací. V devadesátých letech minulého století bylo zapotřebí nahradit starý šifrovací standard DES (Data Encryption Standard), který již neposkytoval potřebnou bezpečnost.

V roce 1997 bylo americkým NIST (National Institute of Standards and Technologie – Národním institutem standardů a technologií) vypsáno výběrové řízení na symetrický šifrovací algoritmus pro ochranu citlivých dat ve státní sféře. Byl vybrán šifrovací algoritmus Rijndael pocházející od tvůrců z Belgie.

Standard AES připouští klíče délek 128, 192 a 256 bitů. Nejvyšší délka klíče 256 bitů byla americkou NSA (National Security Agency) doporučena k ochraně dat klasifikovaných jako „přísně tajné".[15]

3.5.7 RADIUS Server

RADIUS poskytuje tři síťové služby známé jako AAA (Authentication, Authorization and Accounting - autentizace, autorizace a účetnictví). Tyto služby umožňují síťovým správcům jednoduchý způsob k:

- Identifikaci vzdálených uživatelů a kontrolu přístupu uživatelů do sítě. (autentizace).
- Definici, co který uživatel smí, řízením přístupu k síťovým zdrojům (autorizace).
- Sledování, ke kterým zdrojům uživatel přistoupil z důvodů účtování za služby (účetnictví).

RADIUS klient obsahuje Network Access Server (NAS), který poskytuje jednomu nebo více vzdáleným uživatelům přístup k síťovým zdrojům. Jediný RADIUS server je schopen obsloužit několik stovek RADIUS klientů a až několik desítek tisíc koncových uživatelů. Pro případ poruchy nebo nedostupnosti prvního RADIUS serveru se ve velkých sítích zadává adresa jednoho nebo i více alternativních RADIUS serverů.

Procedura přihlašování v RADIUS serveru kombinuje autentizaci a autorizaci za účelem poskytnutí větší bezpečnosti.

Autentizace je nezbytná a zahrnuje zadání uživatelského jména a hesla. Je to proces, kterým je ověřována identita přihlašujícího se uživatele. RADIUS podporuje mnoho autentizačních protokolů včetně PAP (Password Authentication Protocol) a CHAP (Challenge Handshake Authentication Protocol) nebo třeba přihlašování v systému Unix. K předejití průniku potencionálního útočníka do sítě, RADIUS server šifruje uživatelské heslo pro přenos mezi klientem a serverem.

Autentizační RADIUS server odpoví na požadavek od známých klientů a zamítne požadavky od neznámých klientů. Před autentizováním jakéhokoliv uživatele musí NAS ověřit svou vlastní identitu autentizací s RADIUS serverem. K tomuto účelu slouží sdílené tajemství (Shared Secret).

Shared Secret je textový řetězec nakonfigurovaný na straně RADIUS klienta i serveru a není nikdy poslán skrz síť v jeho otevřené (nezašifrované) podobě. Během autentizace RADIUS server vyšle náhodná čísla k NAS, která jsou zkombinována za použití hashovacího algoritmu MD5 s Shared Secret. Tímto způsobem vzniklý blok dat je odeslán zpět na RADIUS server. Ten následně ověří pravost zprávy za pomocí vlastní kopie Shared Secret. NAS odpojí všechny uživatele, kteří se nebyli schopni úspěšně autentizovat s RADIUS serverem.

Autorizace je proces restrikcí a povolení, tzn. co je uživateli v síti zakázáno a co je dovoleno. RADIUS server je zodpovědný za znalost, které služby a privilegia jsou přiděleny oprávněným uživatelům a vrací tuto informaci komunikačnímu serveru v případě, že tato autorizace proběhne úspěšně.

Účetnictví je proces sběru dat a podávání statistických údajů. Účetnický server RADIUS sbírá a ukládá statistiky poslané RADIUS klienty a v případě požadavku klienta je mu tato statistika zaslána. Tato data obsahují:

- Délku uživatelova přihlášení
- Počet paketů, který byl přijat a odeslán
- Počet přijatých a odeslaných bajtů
- Různé jiné statistické informace

Těchto informací může být například využito pro vystavení účtu za služby klientovi, výkonnostní analýzu provozu dat v síti nebo při odstraňování problémů v síti.[3, 9]

3.6 Útoky na bezpečnost sítě

Existuje celá řada zabezpečovacích mechanismů Wi-Fi sítí (WEP, WPA, WPA2 apod.), avšak existuje i celá řada útoků na bezpečnost a integritu sítě. Důvody k takovémuto útoku mohou být od pouhé zvědavosti, přes různé pokusy vlastnit zdarma internetové připojení skrze slabě zabezpečenou Wi-Fi síť až po velice závažné útoky např. průmyslovou špionáž mezi firmami. Jeden z typů útoků je DoS (Denial of Service). [12, 13]

3.6.1 Útok typu DoS

Cílem útoku typu DoS je znefunkčnění serveru poskytujícího určité služby. DoS využívá k útoku žádosti o spojení SYN (connection synchronization). K útoku stačí

pouze jeden nebo několik počítačů. Jde o tzv. útoky typu SYN flood. Z útočících počítačů je vysílán falešný požadavek na zaházejí spojení (SYN). Cílový server vyšle odpověď ACK (acknowledgement), na kterou však již neobdrží žádnou odpověď. Cílový server je ovšem nastaven tak, aby držel linku otevřenou po předem definovaný časový úsek. Pokud server neobdrží včas odpověď, linku uzavře. V případě, že požadavků SYN přijde velké množství, server má otevřené velké množství spojení a není schopen obsloužit další uživatele. Server jen čeká na odpovědi a neobsluhuje nikoho, protože není schopen otevřít žádná další spojení. Jelikož je server zahlcen falešnými požadavky, není schopen uspokojit potřeby skutečných uživatelů Proti útokům typu SYN flood se dá bránit pomocí specifického nastavení firewallu[8]. Povolíme pouze n-SYN packetů za sekundu z jedné IP adresy. [12, 13]

3.6.2 Man in the Middle

Útoky typu Man in the Middle (muž uprostřed) fungují na principu, že útočník vstoupí mezi přístupový bod a klienta a odposlouchává přenášená data. Útočník v první fázi útoku shromažďuje informace o účastnících komunikace (klientu a přístupovém bodu) jako je například SSID přístupového bodu, MAC adresa uživatele. Jakmile útočník získá dostatek informací, přeruší veškerou komunikaci mezi uživatelem a přístupovým bodem. Útočník je schopen s informacemi, které získal, vytvořit falešný přístupový bod a změnit připojení uživatele z původního přístupového bodu na podvržený přístupový bod. Data, která na tento přístupový bod přijme, zaznamenává a také přeposílá na skutečný přístupový bod. Jak klient, tak přístupový bod se domnívají, že jejich komunikace probíhá přímo, zatímco ve skutečnosti jejich komunikaci zprostředkovává a zachytává útočník (muž uprostřed). Útočník je tak schopen se dostat ke všem datům včetně hesel a různých citlivých dat.[12, 13]

3.6.3 Obrana

Útoky tohoto typu patří k těm náročnějším na provedení, avšak v dnešní době existuje celá řada programů na internetu k provedení útoku „muž uprostřed". Proto se

[8] Firewall [online]. 2008 [cit. 2009-05-04]
Dostupný z WWW: <www.fwbuilder.org/docs/UsersGuide.pdf>

jej v bezpečnosti sítě nesmí opomenout. Dobrou obranou je používat obousměrný autentizační mechanismus za využití důvěryhodné třetí strany např. RADIUS serveru. Rovněž je dobré mít podrobnou radiovou mapu sítě a pravidelně zkontrolovat ručně, zda nevysílá nějaký přístupový bod, který v plánu nefiguruje. Mohl by to být právě podvržený přístupový bod. [12, 13]

4 ANALÝZA PROBLÉMU A SOUČASNÉ SITUACE

Výrazný pokles cen v oblasti bezdrátových adaptérů umožnil plošné rozšíření bezdrátových infrastruktur, ať už do podnikové sféry nebo do domácností. Bezdrátová síť usnadňuje uživatelům práci. Data jsou dostupná kdekoliv v pokryté oblasti.

Avšak bezdrátová síť s sebou přináší i množství nevýhod a bezpečnostních rizik. V případě nějaké malé domácí či firemní sítě s několika přístupovými body není návrh a administrace takové sítě velkým problémem. Ale v případě projektu rozsáhlé firemní sítě se můžeme setkat s problémy jako například:

- opětovná autorizace při přemístění se k jinému přístupovému bodu
- složitý dohled nad všemi prvky infrastruktury sítě
- nerovnoměrné pokrytí signálem
- zabezpečením sítě proti úniku informací nebo narušení její funkčnosti.

4.1 Bezpečnost bezdrátové sítě

Při budování bezdrátové sítě nestačí pouze zabezpečení samotného bezdrátového signálu, který se šíří vzduchem. Je také potřeba fyzicky chránit přístupové body a totéž platí i pro zbytek infrastruktury sítě.

Obecně se dá říci, že bezpečnost sítě je často přímo úměrná ceně zařízení a nepřímo úměrná výkonu sítě, jednoduchosti obsluhy a administrace sítě. Proto při výběru vhodného zabezpečení musíme mít na paměti, k jakému účelu bude síť využívána. Těžko si lze představit, že pro malou domácí síť budeme například využívat autorizační server RADIUS. Náklady pro vybudování takto zabezpečené infrastruktury by byly enormní a také nároky na administraci by byly příliš vysoké. U jednoduché sítě je přínosem i nepříliš bezpečný WEP. Pro zkušenějšího útočníka by nebyl problém prolomit toto zabezpečení, ale stálo by ho to čas a úsilí. Pravděpodobnost zisku nějakých cenných dat a informací je u domácí sítě relativně malá. Z tohoto důvodu by i WEP odradil většinu útočníků, kteří by si našli snadnější cíl, síť bez jakéhokoliv zabezpečení. Přístupových bodů bez jakéhokoliv zabezpečení existuje v dnešní době

stále velké množství. Pokud by se však jednalo o nějakou firmu, zde použití WPA, nebo lépe WPA2 je nutností. U takové sítě je předpoklad výskytu citlivých a potencionálně cenných dat vysoký, a proto i nebezpečí útoku na takovou síť je mnohem vyšší.

4.2 Analýza světové bezpečnosti bezdrátových sítí

„Průzkum, který provedla agentura Vanson Bourne, zjistil, že více než polovina velkých společností používá stejné bezpečnostní opatření pro kabelové i bezdrátové sítě. Přestože kabelové i bezdrátové LAN sítě čelí různým typům ohrožení a mají odlišné slabé stránky, pouze 47 % společností používá na svých bezdrátových sítích kódování WEP nebo WPA, a méně než třetina (30 %) používá nějakou formu ochrany proti průniku do bezdrátových sítí.

IT oddělení v dnešní době čelí mnoha rozdílným bezpečnostním problémům bezdrátových sítí. Například 79 % organizací se snaží podporovat vhodné bezpečnostní metody tím, že používají stejné IT postupy v rámci celé organizace. Nicméně výzkum rovněž zjistil, že 51 % společností nemá žádný způsob, jak ve své síti tyto postupy prosazovat. Velkým problémem současnosti je mobilita pracovníků, kteří se připojují do firemní sítě z veřejně dostupných internetových sítí. 56 % společností se domnívá, že mnoho zaměstnanců porušuje bezpečnostní opatření tím, že zasílá firemní data přes naprosto nezabezpečené bezdrátové sítě, jako jsou bezdrátové hotspoty v kavárnách namísto toho, aby používali nějakou formu VPN.“ [9]

[9] Převzato z [19]

5 VLASTNÍ NÁVRH ŘEŠENÍ

Projekt je vypracován pro střední školu Garance, o.p.s se sídlem ve Znojmě. Nosnou myšlenkou projektu je přechod od klasické výuky k výuce s podporou počítačů. Výsledkem projektu bude postupné zapojení studentů školy do výuky s podporou počítačů - notebookové třídy.

Motivem projektu je zatraktivnit studium pro studenty, práce s počítačem je pro studenty podstatně zajímavější a efektivnější, než klasické nudné mentorování.

V současné době nastává dvojí trend ve společnosti, na jedné straně rapidně ubude studentů, na druhé straně jsou stále větší požadavky na odborníky nejrůznějších profesí, vzroste potřeba vysoce kvalifikovaných pracovníků.

Současná škola je pro studenty málo motivující, nejsou využity potenciály nadějných žáků, naopak žáci či studenti potřebující ke zvládnutí studia více času, nezvládají dostatečně látku, mají špatný prospěch a časem jsou také bez další motivace ke studiu. V současné době přibývá studentů s různými poruchami učení, kteří vyžadují individuální přístup a pro které je klasická výuka nevhodná. Zvláštní skupinu studentů pak tvoří zahraniční studenti, či děti přistěhovalců, kteří potřebují postupně zvládnout výuku v pro ně cizím nebo ne zcela zvládnutém jazyce. Individuální přístup ke studentům přináší při klasické výuce nezvládnutelné situace, výsledkem je, že nadaní studenti se časem nudí, ztrácejí motivaci a upadají do průměru. Naopak pro pomalejší studenty začne být probíraná látka nepochopitelná, protože nezvládli látku předcházející.

Současný převratný vývoj v oblasti výpočetní techniky umožňuje řadu dříve těžko zvládnutelných situací ve výuce usnadnit. Došlo k velkému pokroku jednak v oblasti HW tak i SW a tento vývoj stále rychlým tempem pokračuje. Výkony počítačů umožňují pracovat s náročnými programy, multimediální aplikace jsou již naprosto běžné. Prudký vývoj je i v oblasti systémů rozpoznávajících řeč, které jsou perfektní např. pro výuku jazyků. Dalším předpokladem pro výuku je dostatečně rychlé neomezené připojení na internet. I v této oblasti jde vývoj rychle dopředu – přenosová kapacita se zvyšuje, ceny klesají. Obdobná situace je i v oblasti datových projektorů, či

interaktivních tabulí, notebooků. Všeobecně se předpokládá, že ceny HW budou nadále velmi příznivé a budou klesat.

Na velkých školách je realizace výše uvedené myšlenky zatím složitým technickým problémem vzhledem k počtu počítačů v síti. Na škole Garance lze tento problém technicky a finančně vyřešit, protože se jedná o malou školu a počty počítačů budou narůstat zvládnutelných tempem.

Realizace projektu vyžaduje splnění řady opatření jak technických, tak i organizačních, projekt musí být realizován v několika na sebe navazujících etapách v průběhu několika let.

Mým úkolem je vybudovat bezdrátovou síť pro účely interaktivní výuky, výběr notebooků a dalších nezbytných komponent, které jsou nepostradatelné pro úspěšné fungování projektu.

5.1 Cíle Projektu

- nákup a umístění přístupových bodů do učeben
- pokrytí 4 učeben Wi-Fi signálem
- vybavení studentů notebooky
- připojení přenosných počítačů do sítě

5.2 Hardware a software používaný v současnosti

Škola využívá na počítačích kancelářské aplikace Microsoft Office 2003. Operační systém je zde použit Microsoft Windows XP Professional edition SP3.

Stávající infrastruktura obsahuje Wi-Fi přijímač od společnosti Skynet. Pracuje v pásmu 5 Ghz a společnost poskytuje internet o rychlosti 8 Mbit/s. Směrovač Cisco 1600 je zapůjčen od poskytovatele internetového připojení. Ten je propojen s přepínačem (Edimax - 5 portů) pomocí UTP kabelu s koncovkami RJ-45. Směrovač a přepínač Edimax jsou umístěny v ředitelně. Z ředitelny je vedena metalická kabeláž propojující přepínač Edimax s dalšími dvěma přepínači. První z nich je SMC EZ

6516TX a poskytuje připojení do sítě pro počítačovou učebnu a druhý je LINKSYS - SD216, který zajišťuje připojení sborovny.

Cílem mého návrhu je vybudovat bezdrátovou síť ve 4 učebnách pro vytvoření kvalitních podmínek pro interaktivní výuku. Studentům bude zakoupen notebook s Wi-Fi kartou podporující standard 802.11g. Notebooky zůstanou majetkem školy z důvodů správy sítě a jejího zabezpečení.

5.3 Fáze realizace projektu

- návrh přístupových bodů v učebnách
- výběr vhodných zařízení
- nákup speciálního nábytku do učebny
- realizace přípojných míst do učeben
- úpravy elektrické instalace
- nastavení bezdrátových přístupových bodů v učebnách
- zabezpečení sítě
- připojení přístupových bodů do páteřní sítě
- zajištění stálé konektivity v síti

5.3.1 Návrh přístupových bodů v učebnách

Síť bude využívat standard 802.11g. Tento standard pracuje v bezlicenčním pásmu 2,4 Ghz. Jeho rychlost je 54 Mbit/s. V České republice je možnost nastavení až 13 různých kanálů. Šířka jednoho kanálu je 22 MHz, ovšem bezlicenční pásmo má šířku pouze 83,5 Mhz. Proto v praxi jsou v jedné lokalitě použitelné pouze 3 kanály.

Wi-Fi signálem je potřeba pokrýt čtyři učebny. Proto do každé učebny bude umístěn jeden přístupový bod, který bude zajišťovat pokrytí signálem v dané třídě.

Nepřekrývající se frekvence však jsou pouze tři, tento problém bude vyřešen umístěním dvou přístupových bodů na stejném kanálu na opačný konec chodby. Pokud by rušení existovalo, musel by se upravit výkon vysílačů bezdrátové sítě.

5.3.2 Výběr vhodných zařízení

Přístupový bod jsem vybral WNR 3500 od společnosti Netgear. Jedná se o renomovaného výrobce. WNR 3500 podporuje až gigabitový Ethernet a nejmodernější standard 802.11n Draft2. Samozřejmostí je podpora starších standardů 802.11b/g. Tato komponenta by se mohla využít i v budoucnosti při případném přechodu u páteřní sítě na rychlost 1 Gb/s. Směrovač zajišťuje spolehlivou podporu hlasových, internetových či video aplikací a umožňuje uživatelům souběžně vyhledávat na internetu, streamovat video ve vysokém rozlišení i pracovat s elektronickou poštou.

V ředitelně je umístěn 5-ti portový přepínač Edimax. Tento přepínač je propojen ze směrovačem Cisco 1600 a poskytuje připojení k internetové síti pro počítačovou učebnu a sborovnu. V rámci projektu je třeba jej vyměnit. Prvním důvodem je nedostatek portů pro připojení 4 nových přístupových bodů. Druhým důvodem je enormní zvýšení zátěže při připojení všech klientů. Z tohoto důvodu zde byl vybrán relativně drahý přepínač Cisco Catalyst 2940.

Při výběru notebooků byly ředitelem školy vzneseny následující požadavky: alespoň 15-ti palcový monitor, dostatečný výkon pro používané aplikace, DVD mechanika a samozřejmě bezdrátový adaptér. Vybral jsem notebooky Hewlett Packard 550, protože splňují zadané požadavky a mají příznivý poměr ceny a výkonu. Jejich specifikace je uvedena v tabulce 5.1. Procesor je založen na moderní Core 2 architektuře poskytující dostatečný výkon pro výukové aplikace. V případě potřeby může být operační paměť rozšířena ze současných 2 GB až na 4 GB, což by umožnilo zlepšení výkonu v budoucnosti.

Tabulka 5.1: Technická specifikace HP 550

Procesor	Intel Core 2 Duo (T5670)
Frekvence procesoru	1,8 Ghz
Operační paměť	2048 MB RAM
Pevný disk	250 GB
Mechanika	DVD±RW+DL-RAM LightScribe
Velikost displeje	15,4
Rozlišení displeje	WXGA 1280 x 800
Grafická karta	Intel Graphics Media Accelerator X3100

Zdroj[10]

[10] HP 550 [online]. 2009 [cit. 2009-05-04]
Dostupný z WWW: <http://www.alza.cz/hp-550-d97836.htm>

5.3.3 Nákup speciálního nábytku do učebny

Interaktivní výuka nebude probíhat každou vyučovací hodinu, proto byl dalším požadavkem učitelského sboru výběr specifického nábytku do učeben. Nábytek bude sloužit nejen jako stojan pro notebook, ale bude možné kdykoliv notebook přemístit dovnitř stolu a tak rychle přejít ke klasické výuce. Ukázky z praxe jsou uvedené na obrázcích v příloze č.3.

5.3.4 Realizace přípojných míst do učeben

K připojení přístupových bodů s přepínačem Cisco bude použita UTP kabeláž s koncovkami RJ-45. Kabely budou vedeny po omítce chodbou v lištách.

Přístupové body budou uloženy v uzamčených skříních. Učebny jsou již těmito skříněmi vybaveny, využívají se pro uložení videopřehrávačů. Napájení je zde již připraveno pro televizi a jiná elektrická zařízení.

5.3.5 Úpravy elektrické instalace

V učebnách je nutné zvýšit počet elektrických zásuvek. Vedení bude řešeno podokenními plastovými lištami a klasickými dvojzásuvkami. Nebude zapotřebí zvyšovat kapacitu rozvodné skříně, škola má v současnosti již dostatečnou elektrickou infrastrukturu.

5.3.6 Nastavení přístupových bodů

Název SSID bude odpovídat číslům učeben (Ucebna 1-4) a bude vypnuto jeho vysílaní. Pro zamezení neautorizovaných přístupů do směrovače bude nastaveno nové uživatelské jméno a bezpečné alespoň 12-ti místné heslo. Oprávněn ke změnám v nastavení sítě bude pouze správce sítě. Pro případ nouze bude heslo uloženo na bezpečném místě.

5.3.7 Zabezpečení sítě

Od charakteru dat se bude odvíjet i úroveň zabezpečení celé sítě. Jelikož se jedná o data související s výukou studentů střední školy, není zde důvod využít

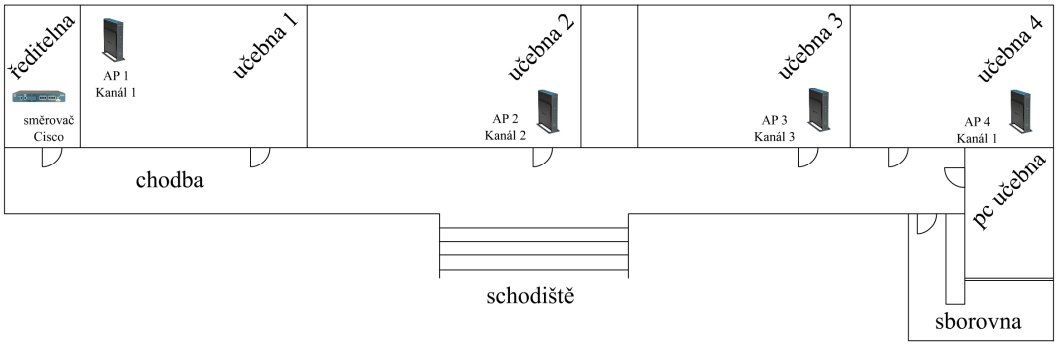
komplexní a zbytečně drahé zabezpečovací metody jako je například WPA2 enterprise. V této síti nehrozí bezprostřední únik citlivých dat. Pro zajištění integrity sítě a pro znesnadnění průniku do sítě případnými útočníky bude využit standard WPA se šifrováním AES.

Notebooky budou připojeny do internetové sítě. Je potřeba zabezpečit počítače proti virům a ostatnímu škodlivému softwaru. Zabezpečení bude realizováno antivirovým programem AVG v aktuální verzi, jehož multilicenci již v současnosti škola vlastní.

Úkolem projektu je vytvářet prostředí pro interaktivní výuku. K dosažení tohoto cíle je potřeba mimo jiné učinit represivní opatření zamezující studentům vykonávat práci na počítačích bez učitelského dohledu. K tomuto cíli bude zakoupen program Vision 6 (dříve MasterEye), který umožňuje aktivní monitorování studentských PC, dohled nad prací studentů na internetu, uzamykání klávesnic, dálkové řízení počítačů v síti, distribuci souborů, jejich rozesílání a sběr, spouštění programů a otevírání www stránek na dálku z učitelského PC.

5.3.8 Zajištění stálé konektivity v síti

Stálé připojení k internetu bude v síti zajištěné páteřní sítí. Prvky páteřní sítě obsahují AP Cisco a 4 AP Netgear. AP Cisto od společnosti Skynet bude propojen s přepínačem v ředitelně a následně rozveden pomocí UTP kabeláže do každého ze 4 přístupových bodů Netgear v učebnách. Schéma je uvedeno na obrázku 5.3.



Obrázek 5.1: Schéma rozmístění síťových prvků

5.4 Náklady na projekt

Tabulka 5.2: Náklady na projekt

Položka	počet kusů	orientační cena s DPH za kus	orientační celková cena s DPH
Notebook HP 550	25	12 602 Kč	315 050 Kč
Switch Cisco	1	11 958 Kč	11 958 Kč
Netgear WNR3500	4	3 800 Kč	15 200 Kč
Vision 6.7	1	25 764 Kč	25 764 Kč
Speciální nábytek	25	3 200 Kč	80 000 Kč
			447 972 Kč

Hlavní část nákladů bude tvořit nákup notebooků. A dále vybavení učebny nábytkem a nákup softwaru. Za výslednou cenu přibližně 450 000 Kč škola získá potřebné vybavení a infrastrukturu pro projekt interaktivní výuky. Projekt by byl spolufinancován školou z vlastních zdrojů a studenty formou školného.

5.5 Přínosy navrhovaného řešení

Velikou předností je respektování individuálních potřeb žáků při výuce, což je ve školství novodobý trend. Zlepšit by se díky interaktivní měla výuce motivace žáků ke studiu. V neposlední řadě by projekt měl zlepšit i integraci zahraničních studentů nebo studentů s různými postiženími v kolektivu třídy.

Těchto cílů může vyučující dosahovat uspořádáním učebny a nově by také mohl manipulovat i s rozmístěním počítačů. Notebooky mají oproti stolním počítačům výhodu v tom, že jsou po určitou dobu nezávislé na dodávce elektrického proudu. Proto je možná rychlá změna uspořádání třídy. K této mobilitě bude přispívat vybudovaná infrastruktura Wi-Fi sítě. Další výhodou je spotřeba elektrické energie u notebooků, která je několikanásobně nižší než u stolních počítačů. V učebně s 15 průměrnými stolními počítači, které jsou v provozu 8-10 hodin denně, činí rozdíl přibližně 20 000 Kč za jeden rok.

6 ZÁVĚR

Bezdrátové technologie nás začínají obklopovat na každém kroku. Jejich počet roste rychlým tempem díky snižujícím se cenám. Pronikají do firemního i domácího prostředí a poskytují řadu výhod, které jsem již předestřel v úvodu. Bohužel s šířením dat vzduchem vzrostlo riziko úniku citlivých dat, proto je třeba dbát i na řádné zabezpečení sítě. Avšak vynaložené prostředky na ochranu dat by vždy měly být nižší, než jaká je samotná hodnota přenášených dat.

Šifrování WEP by se nemělo v praxi vůbec používat. WEP nijak neřeší vytváření nových klíčů a jejich distribuci. Alternativou je WPA a WPA2. WPA2 enterprise nabízí silné a kvalitní zabezpečení vhodné i pro sítě, kde jsou přenášena citlivá data.

Projekt interaktivní výuky ve školách je velice zajímavý nápad a v současné době je jeho realizace proveditelná díky klesajícím cenám elektroniky. Vytvoření interaktivní výuky za podpory notebooků získá škole také prestiž. Schopnost školy poskytnout interaktivní formu výuky zajistí škole dostatečný počet studentů i v dnešní době, kdy počet studentů neustále klesá. Přinese nové možnosti výuky a je schopen napomoci integraci zahraničních žáků nebo žáků s nějakým postižením.

SEZNAM POUŽITÉ LITERATURY

[1] BARKEN, Lee. *Wi-Fi : jak zabezpečit bezdrátovou síť*. Vyd. 1 Brno : Computer Press 2004. 174s. ISBN 80-251-0346-3

[2] BRISBIN, Shelly. *Wi-fi : postavte si svou vlastní wi-fi síť*. Praha : Neocortex, 2003. 248 s. ISBN 80-86330-13-3

[3] HASSELL Johnatan. *RADIUS*. O'Reilly, ISBN 0-596-00322-6

[4] MOLNÁR, Zdeněk. *Efektivnost informačních systémů*. Vyd. 1 Praha: Grada, 2000, 142s. ISBN 80-7169-410-X.75

[5] PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace*. Vyd 1. Brno : Computer Press, 2005, 179s. ISBN 80-251-0791-4

[6] ZANDL, Patrick. *Bezdrátové sítě WiFi : praktický průvodce*. Vyd. 1. Brno : Computer Press, 2003. 190 s. ISBN 80-7226-632-2

[7] 802.11n [online]. 2007 [cit. 2009-05-04]. Dostupný z WWW: <http://www.networkworld.com/community/node/20368>

[8] 802.X autentication and Extensible autentication protocol [online]. 2003 [cit. 2009-05-04]. Dostupný z WWW: <http://www.foundrynet.com/pdf/wp-8021x-authentication-eap.pdf>

[9] About RADIUS [online]. 2004 [cit. 2009-05-04]. Dostupný z WWW: <http://www.patton.com/technotes/ras_about_radius.pdf>

[10] Architektura Wi-Fi sítí [online]. 2004 [cit. 2009-05-04]. Dostupný z WWW: <http://www.earchiv.cz/b07/b0500001.php3>

[11] Bezpečnost Wi-Fi - WEP WPA a WPA2 [online]. 2006 [cit. 2009-05-04]. Dostupný z WWW: <http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_CZ.pdf>

[12] Denial of Service útoky: man in the middle, distribuované DoS [online]. 2006 [cit. 2009-05-04]. Dostupný z WWW: <http://www.lupa.cz/clanky/denial-of-service-utoky-vyuziti-mitm-utoku/>

[13] DoS: odmítnutí síťových služeb [online]. 2004 [cit. 2009-05-04]. Dostupný z WWW: <http://www.security-portal.cz/clanky/dos-odm%C3%ADtnut%C3%AD-s%C3%AD%C5%A5ov%C3%BDch-slu%C5%BEeb>

[14] MAC adresa sítí [online]. 2009 [cit. 2009-05-04]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/MAC_adresa>

[15] Moderní šifrování [online]. 2005 [cit. 2009-05-04]. Dostupný z WWW: <www.sms007.cz/index.php?lang=cs&action=download&page=cryptography>

[16] Notebookové učebny – příklady z praxe [online]. 2008 [cit. 2009-05-04]. Dostupný z WWW: <http://www.rvp.cz/clanek/2094>

[17] Přehled doplňků standardu IEEE 802.11 [online]. 2005 [cit. 2009-05-04]. Dostupný z WWW: <http://access.feld.cvut.cz/view.php?nazevclanku=prehled-doplnku-standardu-ieee-802-11&cisloclanku=2005113002>

[18] Sítě ad-hoc [online]. 2007 [cit. 2009-05-04]. Dostupný z WWW: <http://www.marigold.cz/wifi/doku.php/adhoc>

[19] Téměř dvě třetiny organizací zanedbává bezpečnost bezdrátových sítí [online]. 2009 [cit. 2009-05-04]. Dostupný z WWW: <http://computerworld.cz/aktuality/pruzkum-temer-dve-tretiny-organizaci-zanedbava-bezpecnost-bezdratovych-siti-3820>

[20] Weakness in the Key Scheduling Algorithm of RC4 [online]. 2001 [cit. 2009-05-04]. Dostupný z WWW: <http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf>

[21] WEP [online]. 2002 [cit. 2009-05-04]. Dostupný z WWW: <http://www.networkworld.com/details/715.html>

[22] WEP: Dead Again [online]. 2004 [cit. 2009-05-04]. Dostupný z WWW: <http://www.securityfocus.com/infocus/1814>

[23] What is 802.1X [online]. 2002 [cit. 2009-05-04]. Dostupný z WWW: <http://www.networkworld.com/research/2002/0506whatisit.html>

[24] Wi-Fi sítě a jejich slabiny [online]. 2005 [cit. 2009-05-04]. Dostupný z WWW: <http://www.security-portal.cz/clanky/wifi-s%C3%ADt%C4%9B-jejich-slabiny>

SEZNAM POUŽITÝCH ZKRATEK

AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
AP	Access Point
BSS	Basic Service Set
CHAP	Challenge Handshake Authentication Protocol
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
DoS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ESS	Extended Service Set
FHSS	Frequency Hopping Spread Spectrum
FMS	Fluhrer-Mantin-Shamir
IEEE	Institute of Electrical and Electronics Engineers
IVC	Integrity Check Value
LCP	Link-Control Protocol
LEAP	Lightweight Extensible Authentication Protocol
MAC	Media Access Control
MIC	Message Integrity Check
MIMO	Multiple- Input Multiple-Output
NAS	Network Access Server
NIC	Network Interface Conroller
NSA	National Security Agency
OFMD	Orthogonal Frequency Division Multiplexing
PAP	Password Authentication Protocol
PEAP	Protected Extensible Authentication Protocol
PPP	Point-to-Point Protocol
PTMP	Point to Mutipoint
PTP	Point to Point
RADIUS	Remote Authentication Dial In User Service
SSID	Service Set Identifier
TKIP	Temporal Key Integrity Protocol
TLS	Transport Level Security
TTLS	Tunneled Transport Level Security
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2

SEZNAM PŘÍLOH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

Příloha č.1: Dodatky ke standardu 802.11

Doplněk	Rok Schválení	Popis
802.11a	1999	Rychlost až 54Mbit/s v pásmu 5GHz
802.11b	1999	Rychlost až 11Mbit/s v pásmu 2,4GHz
802.11d	2001	Pro země, kde pásmo 2,4GHz není přístupné
802.11c	2003	Mosty (Bridge) mezi přístupovými body
802.11F	2003	Spolupráce přístupových bodů od různých výrobců
802.11g	2003	Rychlost až 54Mbit/s v pásmu 2,4GHz
802.11h	2003	Dynamický výběr kanálu a regulace výkonu
802.11i	2004	Zabezpečování a ověřování mechanismy na MAC vrstvě
802.11j	2004	Využití pásma 4,9 a 5GHz v Japonsku
802.11e	2005	Podpora pro QoS na MAC vrstvě
802.11k	2006?	Měření rádiových prostředků
802.11m	2006?	Revize srandardů
802.11n	2007?	Vysoká propustnost
802.11p	2007?	Bezdrátový přístup pro mobilní zařízení
802.11r	2007?	Rychlý roaming
802.11u	2007?	Spolupráce s externími sítěmi
802.11.2	2008?	Měření a testování WLAN zařízení
802.11v	2008?	Management bezdrátových sítí
802.11s	2008?	Multi-Hopping
802.11w	2008?	Podpora integrity, autenticity, utajení a ochrany dat

Příloha č.2: Notebook HP 550

Obrázek 8.1: HP 550

Příloha č.3: Ukázka nového nábytku v učebně

Obrázek 8.2: Ukázka vybavení učebny 1, převzato z [16]

Obrázek 8.3: Ukázka vybavení učebny 2, převzato z [16]